IPW

PTO/SB/21 (02-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/711,066
Filing Date	2004/8/20
First Named Inventor	Chih-Chiang Wen
Art Unit	
Examiner Name	
Total Number of Pages in This Submission: 3	Attorney Docket Number: MTKP0164USA

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [x] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] After Allowance communication to Technology Center (TC)
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Winston Hsu, Reg. No.: 41,526
Signature	Winston Hsu
Date	8/23/2004

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name			
Signature		Date	

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 0.00

Complete if Known	
Application Number	10/711,066
Filing Date	2004/8/20
First Named Inventor	Chih-Chiang Wen
Examiner Name	
Art Unit	
Attorney Docket No.	MTKP0164USA

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 50-3105

Deposit Account Name: North America Intellectual Property Corp.

The Director is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☐ Credit any overpayments

☑ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 0.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below	Fee Paid
Total Claims		-20** =		X =
Independent Claims		- 3** =		X =
Multiple Dependent				=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 0.00

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	Winston Hsu	*Registration No. (Attorney/Agent)*	41,526	*Telephone*	886289237350
Signature	Winston Hsu			*Date*	8/23/2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereund

申　　請　　日 ： 西元 2004 年 05 月 13 日
Application Date

申 請 案 號 ： 093113416
Application No.

CERTIFIED COPY OF
PRIORITY DOCUMENT

申　　請　　人 ： 聯發科技股份有限公司
Applicant(s)

局　　長
Director General

蔡練生

發文日期： 西元 2004 年 7 月 [illegible] 日
Issue Date

發文字號： [illegible]0320691270
Serial No.

PTO/SB/02B (08-03)
Approved for use through 08/31/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION – Supplemental Priority Data Sheet

Foreign applications:

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
093113416	Taiwan R.O.C.	5/13/2004	☐	☑	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：

※ 申請日期：　　※IPC 分類：

壹、發明名稱：（中文/英文）

指令擷取方法及其系統 /

METHOD AND SYSTEM OF ACCESSING INSTRUCTIONS

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

聯發科技股份有限公司 / MEDIATEK INCORPORATION

代表人：（中文/英文）

蔡明介 / TSAI, MING-KAI

住居所或營業所地址：（中文/英文）

新竹縣新竹科學工業園區創新一路一之二號五樓 / 5F, No. 1-2, Innovation Road 1, Science-Based Industrial Park, Hsin-Chu Hsien, Taiwan, R.O.C.

國　籍：（中文/英文）　中華民國 / TWN

參、發明人：（共 2 人）

姓　名：（中文/英文）

1. 溫志強 / WEN, CHIH-CHIANG
2. 陳炳盛 / CHEN, PING-SHENG

住居所地址：（中文/英文）

1. 310 新竹縣竹東鎮五豐里忠孝街八十五號 / No. 85, Chung-Siao St., Wu-Feng Li, Chu-Dong Town, Hsin-Chu Hsien 310 , Taiwan, R.O.C.
2. 606 嘉義縣中埔鄉隆興村六鄰十三號 / No. 13, Community 6, Lung-Hsing Tsun, Chung-Pu Hsiang, Chia-Yi Hsien 606 , Taiwan, R.O.C.

國　籍：(中文/英文)

1. 中華民國 / TWN
2. 中華民國 / TWN

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：　年　月　日。

◎本案申請前已向下列國家（地區）申請專利 ☐ 主張國際優先權：

【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】

1.

2.

3.

4.

5.

☐ 主張國內優先權(專利法第二十五條之一)：

【格式請依：申請日；申請案號數　順序註記】

1.

2.

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼　順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼　順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

伍、中文發明摘要：

本發明提供一種指令擷取方法及其系統，用來擷取一加密指令。該方法包含有使用一指令擷取控制器來控制該加密指令之存取，使用一微處理器來驅動該指令擷取取控制器以擷取該加密指令，解密該加密指令以產生一解密指令，以及使用該微處理器依據該解密指令執行運算。

陸、英文發明摘要：

A method and a system of accessing encrypted instructions. The method includes utilizing an instruction access controller to access the encrypted instruction, utilizing a microprocessor to drive the instruction access controller to access the encrypted instruction, decrypting the encrypted instruction to generate a decrypted instruction, and utilizing the microprocessor to operate according to the decrypted instruction.

柒、指定代表圖：

(一)本案指定代表圖為：第（ 二 ）圖。

(二)本代表圖之元件代表符號簡單說明：

30	指令擷取系統	32	晶片
34	外部儲存裝置	40	微處理器
42	指令擷取控制器	44	暫存模組
46	解密模組	48	密鑰儲存單元

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

玖、發明說明：

【發明所屬之技術領域】

本發明提供一種指令擷取方法及其系統，尤指一種擷取(access)並解密(decrypt)加密指令(encrypted instruction)以使微處理器(microprocessor)可依據解密指令(decrypted instruction)執行運算的指令擷取方法及其系統。

【先前技術】

在習知光碟機中，一微處理器係擷取儲存於外部記憶體的韌體(firmware)來執行相關運算以控制光碟機的運作，例如最佳功率控制（optimum power control, OPC）與尋軌（track seeking）等，而為了避免在擷取韌體的過程中，韌體的程式碼經由一外部介面而被竊取，所以各種保護外部記憶體所儲存之資料的加密機制已發展來避免上述情形。在習知技術中，儲存於外部記憶體的加密指令係經由外部介面傳輸至一晶片進行解密處理，該晶片內的微處理器再依據解密指令來執行運算，因此，即使加密指令在傳輸過程中被不當竊取，該加密指令所對應的實際程式碼仍無法輕易地被得知。

請參考圖一，圖一為習知指令擷取系統10的示意圖。指令擷取系統10包含有一晶片（chip）12以及一外部記憶體(external memory)14，其中晶片12與外部記憶體14係相互電連接。外部記憶體14係用來儲存加密指令，而晶片12包含有一直接記憶體存取控制器(direct memory access controller, DMA controller)20、一記憶體控制器22、一解密模組24、一儲存裝置26以及一微處理器28。直接記憶體存取控制器20係電連接至記憶體控制器22，用來以一直接記憶體存取模式（DMA mode）來擷取外部記憶體14所記錄的資料，如圖一所示，記憶體控制器22係電連接至外部記憶體14以及解密模組24，因此，在微處理器28不介入控制資料傳輸的

情況下，直接記憶體存取控制器 20 便直接控制記憶體控制器 22，以驅使記憶體控制器 22 自外部記憶體 14 擷取一加密指令並將已擷取的加密指令傳送至解密模組 24。解密模組 24 另電連接至儲存裝置 26，所以當解密模組 24 解密所接收到的加密指令而產生一解密指令時，解密模組 24 便將該解密指令儲存至儲存裝置 26 之中。儲存裝置 26 係電連接至微處理器 28，所以微處理器 28 便可自儲存裝置 26 讀取該解密指令，並執行該解密指令來執行一預定運算。

在習知指令擷取系統 10 之中，晶片 12 係以記憶體分頁(page)為單位以擷取儲存於外部記憶體 14 的加密指令，舉例來說，若外部記憶體 14 中一記憶體分頁係對應 1024 位元，則晶片 12 會控制外部記憶體 14 於一次資料傳輸中將同一記憶體分頁所記錄之 1024 位元的加密資料傳回至晶片 12 中的解密模組 24 來進行相關解密運算，然而，以記憶體分頁為單位的指令擷取系統 10 不但需要較大的頻寬(bandwidth)來傳輸加密指令，也必須使用大容量的儲存裝置 26 來儲存解密指令而造成晶片 12 具有較大的尺寸。除此之外，在習知指令擷取系統 10 中，儲存裝置 26 係使用靜態隨機存取記憶體(SRAM)來儲存解密指令，在晶片 12 的佈局(Layout)中，由於靜態隨機存取記憶體的輸入埠及輸出埠容易被觀察而探測(probe)，因而增加解密指令被竊取的可能性。此外，晶片 12 於讀取加密指令的過程中，其係利用額外之直接記憶體存取控制器 20 來控制加密指令的擷取，因此會增加生產成本，提升電路複雜度，以及造成晶片 12 的尺寸無法有效地降低。

【發明內容】

因此，本發明提供一種可即時解密加密指令並傳送至微處理器以使微處理器可依據解密指令執行運算的指令擷取方法及其系統，以解決上述問題。

根據本發明之申請專利範圍，其係揭露一種指令擷取方法，其包含有

儲存一加密指令，使用一指令擷取控制器來控制該加密指令之存取，使用一微處理器來驅動該指令擷取取控制器以擷取該加密指令，解密該加密指令以產生一解密指令，以及使用該微處理器依據該解密指令執行運算。

本發明之申請專利範圍另提供一種指令擷取系統，其包含有一儲存裝置，用來儲存一加密指令，一指令擷取控制器，電連接於該儲存裝置，用來自該儲存裝置擷取該加密指令，一解密模組，電連接於該儲存裝置，用來解密該加密指令以產生一解密指令，以及一微處理器，電連接至該指令擷取控制器與該解密模組，用來驅動該指令擷取取控制器以控制該儲存裝置將該加密指令傳遞至該解密模組，該微處理器係自該解密模組接收該解密指令以執行運算。

本發明指令擷取方法及其系統可不需使用靜態隨機存取記憶體來暫存擷取出的加密指令，因而可以大幅降低晶片的面積。此外，由於儲存裝置所輸出的加密指令直接傳送至解密模組以產生解密指令，而微處理器便立即依據解密指令來執行運算，因而可降低解密指令被探測的可能性。除此之外，本發明指令擷取方法及其系統並未應用習知直接記憶體存取的機制，因此不需額外設置直接記憶體存取控制器，因此，綜上所述，本發明指令擷取方法及其系統可降低解密指令的被探測，降低生產成本，減少電路複雜度，以及有效降低晶片的尺寸。

【實施方式】

請參考圖二，圖二為本發明第一種指令擷取系統30的示意圖。指令擷取系統30包含有一晶片32以及一外部儲存裝置34，其中晶片32與外部儲存裝置34係相互電連接，而外部儲存裝置34係用來儲存加密指令。晶片32包含有一微處理器40、一指令擷取控制器(instruction access controller, IAC)42、一暫存模組44、一解密模組46以及一密鑰儲存單元48。微處理器40係電連接至指令擷取控制器42，用於驅動指令擷取控制器

42 來擷取指令。指令擷取控制器 42 電連接至外部儲存裝置 34、暫存模組 44 以及密鑰儲存單元 48，用於擷取儲存於外部儲存裝置 34 的加密指令，並控制擷取出的加密指令儲存至暫存模組 44 。密鑰儲存單元 48 係用來儲存一密鑰(key)，而指令擷取控制器 42 可讀取該密鑰以依據該密鑰來解密該加密指令之存取位址(address)。解密模組 46 係電連接至微處理器 40，暫存模組 44，以及密鑰儲存單元 48，解密模組 46 可讀取儲存於密鑰儲存單元 48 中的另一密鑰並根據該密鑰解密儲存於暫存模組 44 的加密指令以產生一解密指令，並將該解密指令傳送至微處理器 40，以使微處理器 40 可依據解密指令來執行運算。

為了詳細描述指令擷取系統 30 的運作方式，請參考圖三，圖三為圖二所示之指令擷取系統 30 的操作流程圖，其包含有下列步驟：

步驟 100：微處理器 40 驅動指令擷取取控制器 42 以擷取加密指令；

步驟 102：指令擷取控制器 42 依據儲存於密鑰儲存單元 48 的密鑰來解密加密指令的儲存位址，並且至外部儲存裝置 34 擷取加密指令；

步驟 104：暫存模組 44 暫存從外部儲存裝置 34 所擷取的加密指令；

步驟 106：解密模組 46 依據儲存於密鑰儲存單元 48 的密鑰來解密儲存於暫存模組 44 的加密指令以產生解密指令；以及

步驟 108：微處理器 40 依據解密指令來執行運算。

本實施例中，外部儲存裝置 34 係為非揮發性記憶體（non-volatile memory)，例如一電子可抹除可程式化唯讀記憶體(electrically erasable programmable read only memory, EEPROM)或一快閃唯讀記憶體(Flash ROM)，而暫存模組 44 係為一揮發性記憶體（volatile memory)，例如由合成電路所產生的 FIFO，另外，密鑰儲存單元 48 亦可至於晶片 32 之外。為了便於說明，本實施例之指令擷取系統 30 係應用於一光碟機，其中外部儲存裝置 34 係用來儲存該光碟機的韌體（firmware)，而晶片 30 即為該光碟機的控制晶片，當該光碟機接收到一電腦主機所發出的高階指令而需進行一尋軌操作來讀取一光碟片上一預定軌道所記錄的資料時，微處理器 40 必

須執行韌體中的尋軌程式碼以控制伺服系統（servo system）執行所需的尋軌操作以移動讀寫頭（pick-up head）至該預定軌道，所以，微處理器40此時便依據尋軌程式碼儲存於外部儲存裝置34的第一儲存位址來驅動指令擷取取控制器42（步驟100），使指令擷取控制器42依據儲存於密鑰儲存單元48的密鑰來解密該第一儲存位址，並且依據該解密之第一儲存位址至外部儲存裝置34擷取加密指令（步驟102）。此外，指令擷取控制器42亦會傳送一第二儲存位址予暫存模組44，用來告知暫存模組44需將外部儲存裝置34所輸出的加密指令暫存於該第二儲存位址(步驟104)。接著，解密模組46便即時地解密暫存於暫存模組44的加密指令，並將一解密指令傳送至微處理器40（步驟106）。最後，微處理器40接收到對應該第一儲存位址之尋軌程式碼的相對應解密指令，並順利地執行該解密指令來執行運算以控制尋軌操作（步驟108）。

當外部儲存裝置34的頻寬是共用時，本發明指令擷取系統30可依據晶片32與外部儲存裝置34之間不同的頻寬需求來調整每次擷取加密指令的數量，當可用頻寬較大時，指令擷取控制器42每次可擷取較多的指令並儲存於暫存模組44，以利用快取的機制來降低指令擷取控制器42進行資料擷取的操作次數來提高微處理器40的運算效率；而當可用頻寬較小時，指令擷取控制器42每次擷取較少的指令並儲存於暫存模組44，因而晶片32便可以使用具有較少儲存容量的暫存模組44來進一步減少晶片32的面積。在可用頻寬極小的情況下，指令擷取控制器42可以每次只擷取一筆加密指令，在此情況下，晶片32亦可完全不使用暫存模組44來作為快取記憶體以暫存外部儲存裝置34所輸出的加密指令，亦即外部儲存裝置34所輸出的一筆加密指令便直接傳送至解密模組46以立即地產生相對應的解密指令。

請參考圖四，圖四為本發明第二種指令擷取系統50的示意圖。指令擷取系統50包含有一晶片52以及一外部儲存媒介56，其中晶片52與外部儲存媒介56係相互電連接。晶片52包含有一密鑰儲存單元58、一微處理器

60、一指令擷取控制器 62、一儲存裝置 64、一暫存模組 66、以及一解密模組 68。請注意，圖四所示之指令擷取系統 50 與圖二所示之指令擷取系統 30 中的同名元件具有相同的功能與運作，因此不再重複贅述，而主要的不同點在於指令擷取系統 50 的儲存裝置 64 係內建(embedded)於晶片 52 中，此外，儲存裝置 64 中所儲存的加密指令係透過指令擷取控制器 62 而由外部儲存媒介 56 所提供，其操作於後詳述。

為了詳細描述指令擷取系統 50 的運作方式，請參考圖五，圖五為圖四所示之指令擷取系統 50 的操作流程圖，其包含有下列步驟：

步驟 120：啟動指令擷取取控制器 62 以擷取儲存於外部儲存媒介 56 的加密指令；

步驟 122：指令擷取取控制器 62 由外部儲存媒介 56 接收加密指令並儲存於儲存裝置 64 之中；

步驟 124：微處理器 60 驅動指令擷取取控制器 62 以擷取儲存於儲存裝置 64 的加密指令；

步驟 126：指令擷取控制器 62 依據儲存於密鑰儲存單元 58 的密鑰來解密加密指令的儲存位址，並且從儲存裝置 64 擷取加密指令；

步驟 128：暫存模組 66 暫存從儲存裝置 64 所擷取的加密指令；

步驟 130：解密模組 68 根據儲存於密鑰儲存單元 58 的密鑰來解密儲存於暫存模組 66 的加密指令以產生一解密指令；以及

步驟 132：微處理器 60 依據該解密指令來執行運算。

本實施例中，外部儲存媒介 56 係為非揮發性記憶體、電腦主機或是硬碟等，而儲存裝置 64 與暫存模組 66 均為揮發性記憶體，例如儲存裝置 64 係為一動態隨機存取記憶體，而暫存模組 66 係為由靜態隨機存取記憶體所構成的快取記憶體，另外，密鑰儲存單元 58 亦可至於晶片 52 之外。同樣地，為了便於說明，本實施例之指令擷取系統 50 係應用於一光碟機，其中外部儲存媒介 56 係用來提供對應該光碟機之韌體（firmware）的加密程式

碼，而晶片 52 即為該光碟機的控制晶片。當該電腦主機開啟而啟動該光碟機時，晶片 52 首先會啟動指令擷取取控制器 62 至外部儲存媒介 56 擷取對應該光碟機之韌體的加密程式碼（步驟 120）。因此，指令擷取取控制器 62 便接收該加密程式碼，並將該加密程式碼所包含的複數個加密指令儲存於儲存裝置 64(步驟 122)。當該光碟機接收到一電腦主機所發出的高階指令而需進行一尋軌操作來讀取一光碟片上一預定軌道所記錄的資料時，微處理器 60 必須執行韌體中的尋軌程式碼以控制伺服系統（servo system）執行所需的尋軌操作以移動讀寫頭（pick-up head）至該預定軌道，所以，微處理器 60 此時便依據尋軌程式碼紀錄於儲存裝置 64 的第一儲存位址來驅動指令擷取取控制器 62（步驟 124），使指令擷取控制器 62 依據儲存於密鑰儲存單元 58 的密鑰來解密該第一儲存位址，並且依據該解密之第一儲存位址至儲存裝置 64 擷取加密指令（步驟 126）。此外，指令擷取控制器 62 亦會傳送一第二儲存位址予暫存模組 66，用來告知暫存模組 66 需將儲存裝置 64 所輸出的加密指令暫存於該第二儲存位址(步驟 128)。接著，解密模組 68 便即時地解密暫存於暫存模組 66 的加密指令，並將一解密指令傳送至微處理器 60（步驟 130）。最後，微處理器 60 接收到對應該第一儲存位址之尋軌程式碼的相對應解密指令，並順利地執行該解密指令來執行運算以控制尋軌操作（步驟 132）。

同樣地，本實施例係利用暫存模組 66 來作為快取記憶體，亦即指令擷取控制器 62 每次可擷取較多的指令並儲存於暫存模組 66，以利用快取的機制來降低指令擷取控制器 62 擷取的延遲次數來提高微處理器 60 的運算效率，而指令擷取控制器 62 亦可每次只擷取一筆加密指令，在此情況下，晶片 52 可完全不使用暫存模組 66 來作為快取記憶體以暫存儲存裝置 64 所輸出的加密指令，亦即儲存裝置 64 所輸出的一筆加密指令便直接傳送至解密模組 68 以立即地產生相對應的解密指令。

請注意，上述實施例中，本發明指令擷取方法及其系統係應用於光碟機中，然而，本發明指令擷取方法及其系統並未侷限於光碟機的應用領域，

其亦可應用於任何需讀取並解譯加密程式碼的裝置，亦屬本發明保護之範疇。

相較於習知技術，本發明指令擷取方法及其系統可不需使用大容量的靜態隨機存取記憶體來暫存擷取出的加密指令，因而可以大幅降低晶片的面積。此外，由於儲存裝置所輸出的加密指令直接傳送至解密模組以產生解密指令，而微處理器便立即依據解密指令來執行運算，因而可降低解密指令被探測的可能性。除此之外，本發明指令擷取方法及其系統並未應用習知直接記憶體存取的機制，因此不需額外設置直接記憶體存取控制器，因此，綜上所述，本發明指令擷取方法及其系統可降低解密指令的被探測，降低生產成本，減少電路複雜度，以及有效降低晶片的尺寸。

以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所作之均等變化與修飾，皆應屬本發明專利之涵蓋範圍。

【圖式簡單說明】

圖式之簡單說明

圖一為習知指令擷取系統的示意圖。
圖二為本發明第一種指令擷取系統的示意圖。
圖三為圖二所示之指令擷取系統的操作流程圖。
圖四為本發明第二種指令擷取系統的示意圖。
圖五為圖四所示之指令擷取系統的操作流程圖。

圖式之符號說明

10、30、50　指令擷取系統
12、32、52　晶片

14	外部記憶體
20	直接記憶體存取控制器
22	記憶體控制器
24、46、68	解密模組
26、64	儲存裝置
28、40、60	微處理器
34	外部儲存裝置
48、58	密鑰儲存單元
42、62	指令擷取控制器
44、66	暫存模組
56	外部儲存媒介

拾、申請專利範圍：

1. 一種指令擷取方法，用於擷取一加密指令(encrypted instruction)，該方法包含有：

使用一指令擷取控制器（instruction access controller, IAC）來控制該加密指令之存取；

使用一微處理器來驅動該指令擷取取控制器以擷取該加密指令；

解密(decrypt)該加密指令以產生一解密指令(decrypted instruction)；以及

使用該微處理器依據該解密指令執行運算。

2. 如申請專利範圍第 1 項所述之指令擷取方法，其中解密該加密指令之步驟另包含有：

提供一暫存模組；以及

依據該指令擷取取控制器所提供之一儲存位址來驅動該暫存模組儲存該指令擷取控制器所擷取之該加密指令。

3. 如申請專利範圍第 1 項所述之指令擷取方法，其另包含有：

設置一密鑰儲存單元，並使用該密鑰儲存單元來儲存一密鑰（key）；

其中解密該加密指令之步驟另包含有讀取該密鑰以及依據該密鑰來解密該加密指令。

4. 如申請專利範圍第 1 項所述之指令擷取方法，其另包含有：

設置一密鑰儲存單元，並使用該密鑰儲存單元來儲存一密鑰（key）；

其中該指令擷取控制器存取該加密指令之步驟另包含有讀取該密鑰以及依據該密鑰來解密該加密指令之儲存位址(address)。

5. 如申請專利範圍第 1 項所述之指令擷取方法，其另包含有：

設置該指令擷取控制器以及該微處理器於同一晶片（chip）上；

其中該加密指令係儲存於一儲存裝置，且該儲存裝置係外接於該晶片。

6. 如申請專利範圍第 1 項所述之指令擷取方法，其中該加密指令係儲存於一儲存裝置，且該指令擷取方法另包含有：

設置該儲存裝置，該指令擷取控制器，以及該微處理器於同一晶片(chip)上。

7. 一種指令擷取系統，其包含有：

一儲存裝置，用來儲存一加密指令(encrypted instruction)；

一指令擷取控制器（instruction access controller, IAC)，電連接於該儲存裝置，用來自該儲存裝置擷取該加密指令；

一解密模組，電連接於該儲存裝置，用來解密(decrypt)該加密指令以產生一解密指令(decrypted instruction)；以及

一微處理器，電連接至該指令擷取控制器與該解密模組，用來驅動該指令擷取取控制器以控制該儲存裝置將該加密指令傳遞至該解密模組，該微處理器係自該解密模組接收該解密指令以執行運算。

8. 如申請專利範圍第 7 項所述之指令擷取系統，其另包含有：

一暫存模組，電連接至該指令擷取控制器、該儲存裝置以及該解密模組，用來依據該指令擷取控制器所提供之一儲存位址來儲存該加密指令，並將該加密指令傳遞至該解密模組。

9. 如申請專利範圍第 8 項所述之指令擷取系統，其中該暫存模組的功能係為一快取記憶體(cache memory)或一緩衝暫存器(FIFO)。

10. 如申請專利範圍第 7 項所述之指令擷取系統，其另包含有：

一密鑰儲存單元，電連接於該解密模組並設置於該晶片外，用來儲存一密鑰（key)；

其中該解密模組係讀取該密鑰以依據該密鑰來解密該加密指令。

11. 如申請專利範圍第 7 項所述之指令擷取系統，其另包含有：

一密鑰儲存單元，電連接於該解密模組並設置於該晶片外，用來儲存一密鑰（key）；

其中該指令擷取控制器係讀取該密鑰以依據該密鑰來解密該加密指令之儲存位址(address)。

12. 如申請專利範圍第 7 項所述之指令擷取系統，其中該指令擷取控制器，該解密模組，以及該微處理器係設置於同一晶片（chip）上，且該儲存裝置係外接於該晶片。

13. 如申請專利範圍第 12 項所述之指令擷取系統，其中該儲存裝置係為非揮發性記憶體（non-volatile memory）。

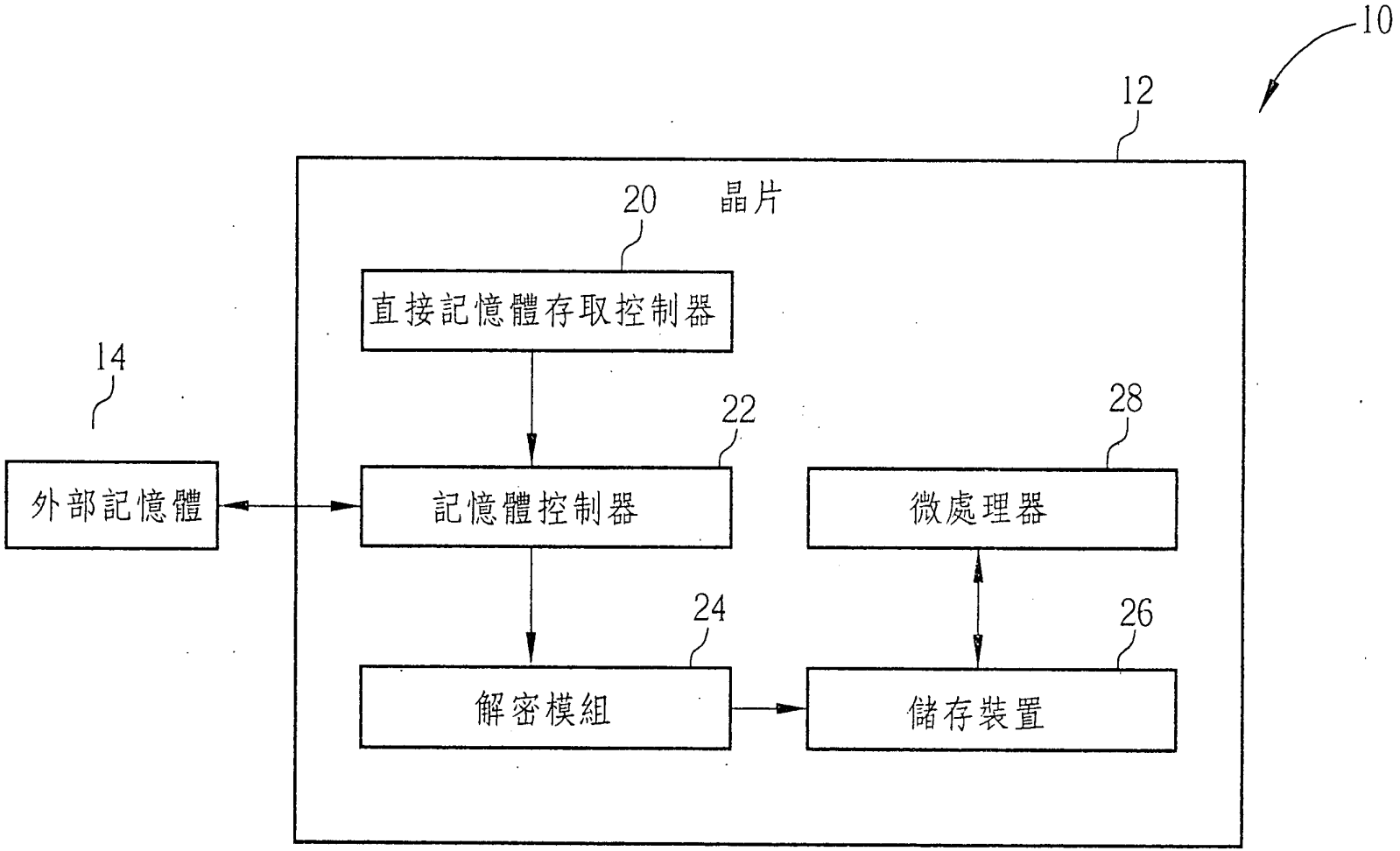
14. 如申請專利範圍第 12 項所述之指令擷取系統，其中該晶片係為一光碟機控制晶片，以及該解密指令係為光碟機韌體(firmware)。

15. 如申請專利範圍第 7 項所述之指令擷取系統，其中該儲存裝置、該指令擷取控制器、該解密模組以及該微處理器係設置於同一晶片（chip）上。

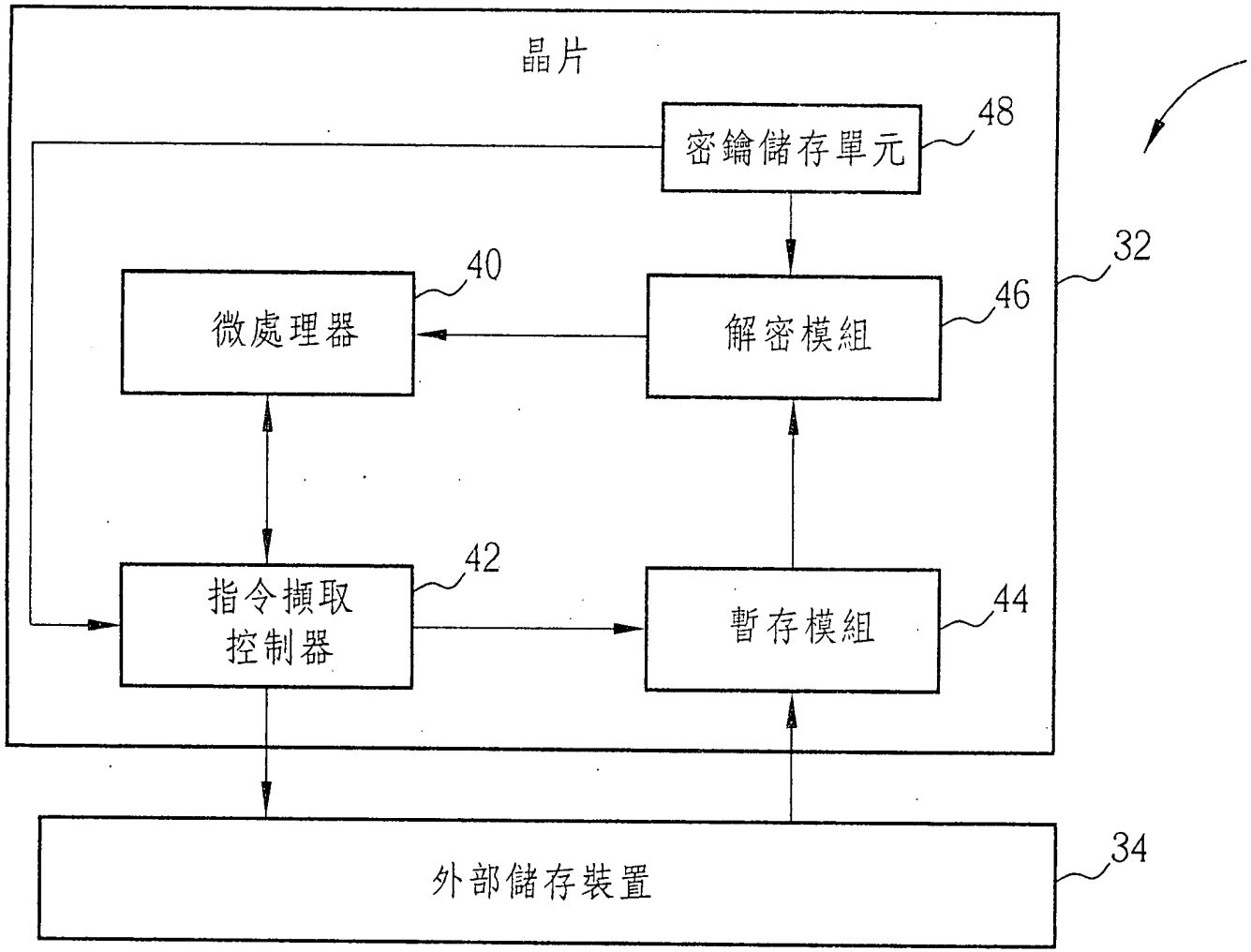
16. 如申請專利範圍第 15 項所述之指令擷取系統，其中該儲存裝置係為揮發性記憶體(volatile memory)。

17. 如申請專利範圍第 15 項所述之指令擷取系統，其中該晶片係為一光碟機控制晶片，以及該解密指令係為光碟機韌體(firmware)。

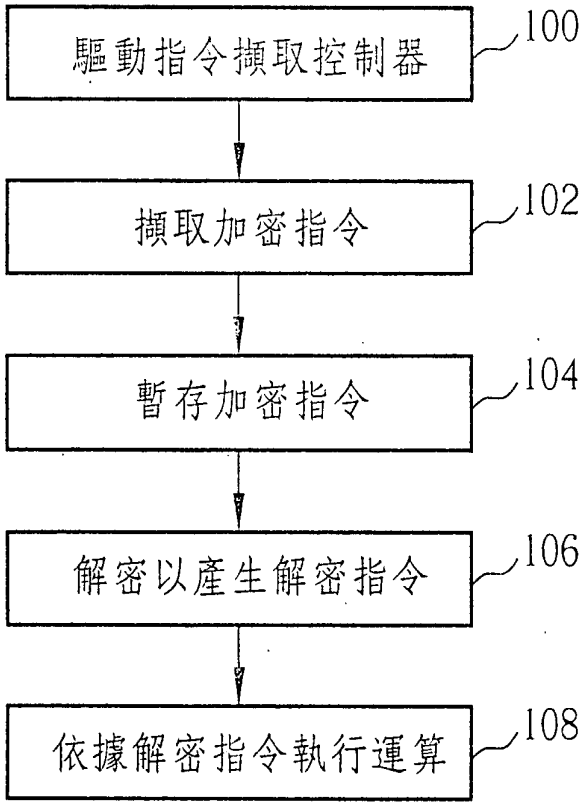
拾壹、圖式：


10
12
晶片
20
直接記憶體存取控制器
14
外部記憶體
22
記憶體控制器
28
微處理器
24
解密模組
26
儲存裝置

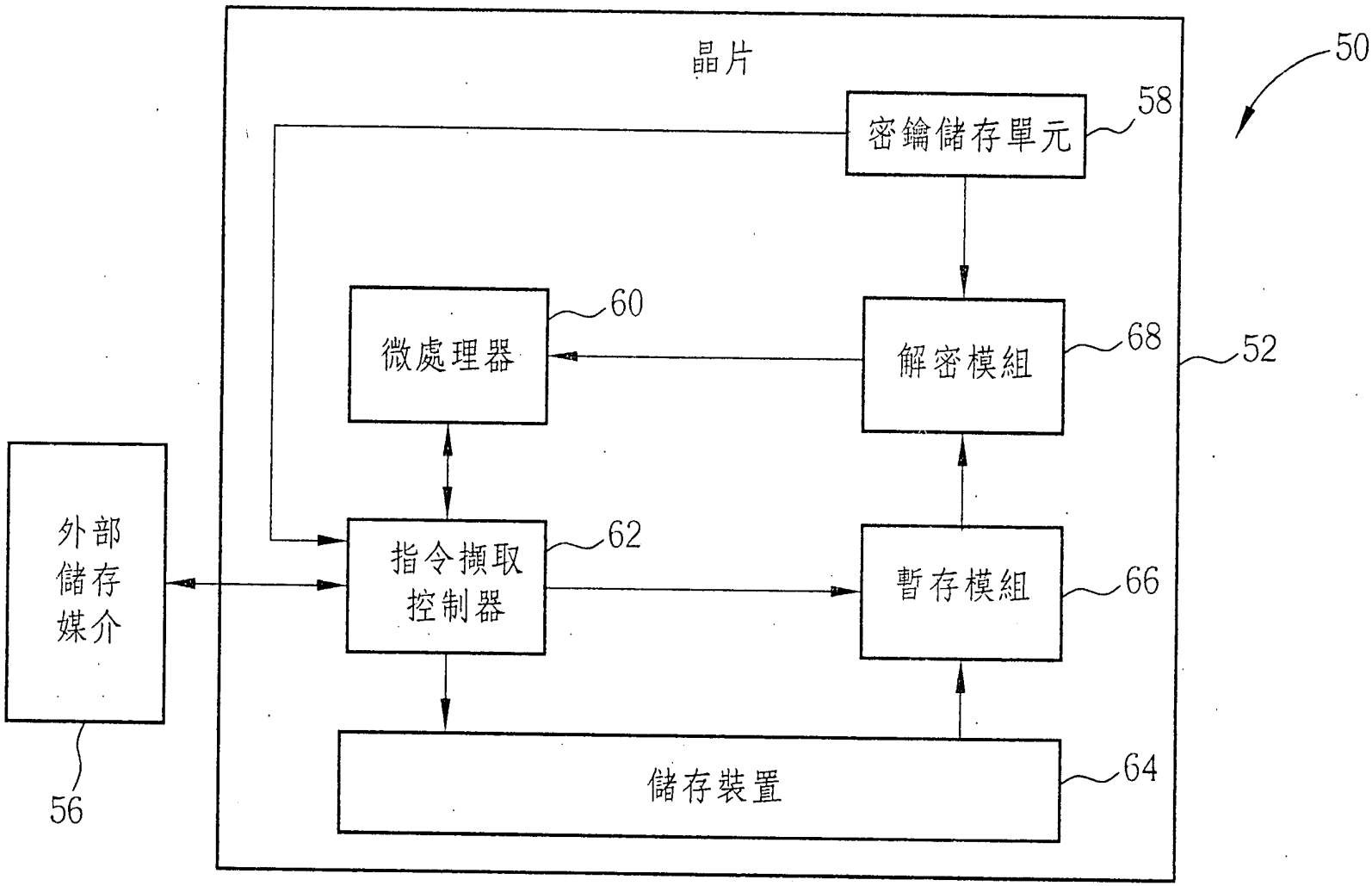
圖一



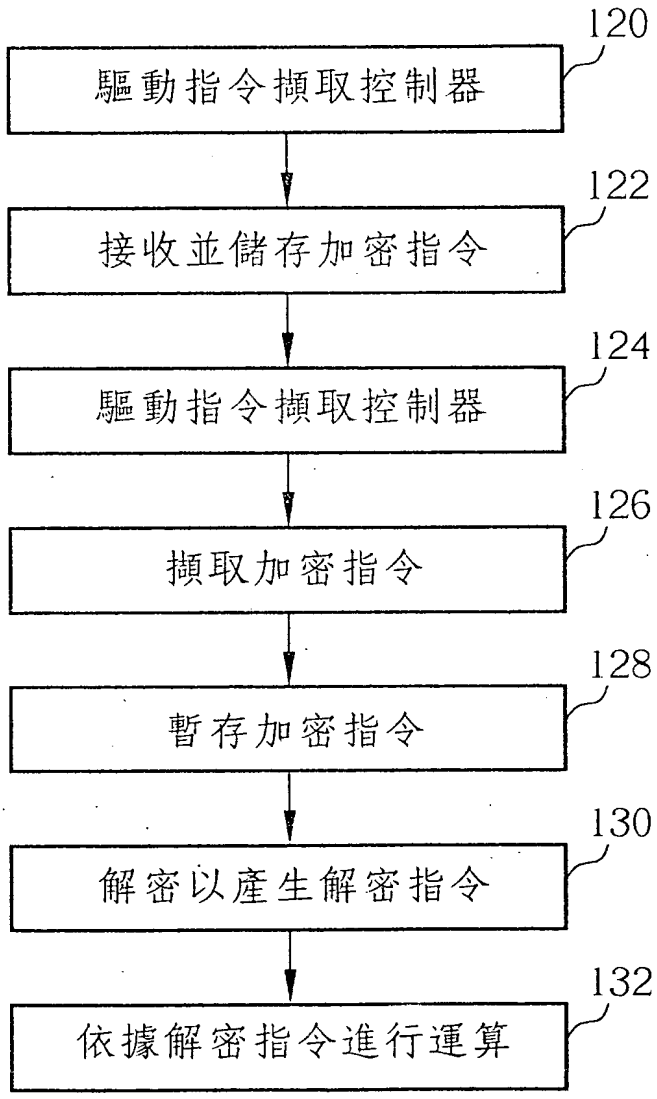
圖二


驅動指令擷取控制器
100
擷取加密指令
102
暫存加密指令
104
解密以產生解密指令
106
依據解密指令執行運算
108

圖三


晶片
50
密鑰儲存單元
58
微處理器
60
解密模組
68
52
外部儲存媒介
指令擷取控制器
62
暫存模組
66
儲存裝置
64
56

圖四


120
驅動指令擷取控制器
122
接收並儲存加密指令
124
驅動指令擷取控制器
126
擷取加密指令
128
暫存加密指令
130
解密以產生解密指令
132
依據解密指令進行運算

圖五